

REMARKS

Initially, Applicants would like to thank the Examiner for acknowledging acceptance of the drawings filed with the present application on September 9, 2003. Applicants would also like to thank the Examiner for acknowledging consideration of each of the documents cited on PTO-1449 forms submitted with Information Disclosure Statements filed on May 26, 2005 and December 12, 2003.

In the outstanding Official Action, the first paragraph of the specification was objected-to, and a requirement was set forth that the "CROSS-REFERENCES TO RELATED APPLICATIONS" section be updated to reflect applications that have matured into patents. Claims 1-3 and 21-23 were rejected under 35 U.S.C. §102(e) over CHEN et al. (U.S. Patent No. 6,061,796). Claims 4-20 and 24-31 were rejected under 35 U.S.C. §103(a) over CHEN in view of BAKER et al. (U.S. Patent No. 5,812,666).

Upon entry of the present amendment, the first paragraph of the specification will have been amended to reflect applications that have matured into patents. Accordingly, Applicants respectfully request reconsideration and withdrawal of the outstanding objection to the specification.

Applicants traverse each of the outstanding rejections. In this regard, CHEN is directed to a system to authenticate parties for server access and communications. In particular, at col. 4, lines 17-27, CHEN discloses "[t]he present invention can be implemented using the existing SmartGATETM system, but adds mutual authentication and encryption services to lower layers by intercepting function calls or data packets and, during initialization of a communications link,

establishing separate channels between the party initiating the communication and the authentication server, and between the authentication server and the party which is to share in the communication, so as to mutually authenticate the parties with respect to the server, and so as to establish a session key which can be used for further direct communications between the parties” (emphasis added).

BAKER is directed to a system for domain authentication for identifying postage meters. In particular, at col. 2, line 61 to col. 3, line 7, BAKER discloses “[i]n accordance with the preferred embodiment of the present invention, **a Key Management System generates and distributes cryptographic keys, such as Vendor keys, USPS keys, and other country's postal keys, to digital meters for multiple domains.** A domain is a logical separation of data and functions enforced by unique **domain authentication** and confidentiality keys. The Key Management System prevents any translation of keys between domains, provides assurance in a domain that the keys were generated in the domain, and that they have been installed in only one meter by the system. The Key Management System securely distributes and maintains cryptographic keys for multiple domains. Further, the Key Management System is structured so that key management for all domains is identical” (emphasis added).

Applicants traverse the rejection of independent claims 1 and 21. In this regard, the Official Action asserts that CHEN discloses features recited in independent claims 1 and 21 at Figs. 6-7, col. 9, lines 42-59 and col. 11, lines 16-49. The Official Action is in error. In this regard, the cited portions of CHEN are directed to a “*client/server response channel used to authenticate the parties and generate the session key*” (col. 11, lines 20—22), and to a method by

which “*each of the parties to the communication is effectively authenticated*” (col. 11, lines 48-49). There is no disclosure of a system that generates a request for a confirmation receipt from a third party authenticator authenticating the attributes of a file as recited in independent claim 1 or the related features of independent claim 21.

Further, at col. 11, lines 24-29, CHEN discloses “[i]n the case of a peer-to-peer application, in which the clients wish to communicate over a direct link 62, the invention provides for the function calls establishing the communications to be intercepted and the initialization procedure routed through channel 61 to the authentication server 23”. However, the above-noted disclosure in CHEN is not a system that generates a request for a confirmation receipt from a third party authenticator authenticating the attributes of a file nor a transferring system that transfers attributes of at least one file to be authenticated to the third party authenticator from the device that requested the confirmation as recited in independent claim 1 or the related features of claim 21.

Additionally, at col. 12, lines 3-6, CHEN discloses “*step 101 is step by which the program 20 addresses the authentication server, step 102 is the step by which the client and server are mutually authenticated*”. Further, at col. 12, lines 13-19, CHEN discloses “*steps 106 and 107 are identical to steps 101 and 102, step 108 is the step by which communications channel 63 shown in FIG. 6 is established, step 109 is the step by which the destination computer authenticated by the server is enabled to decrypt communications received over channel 62, and step 110 is the step by which program 20 encrypts the communications*”. There is no teaching at this portion of CHEN to any transfer of attributes of at least one file to be authenticated to the

third party authenticator as recited in independent claim 1 or the related features recited in independent claim 21.

At col. 11, lines 40-44, CHEN discloses *'the authentication server is thus used to establish a fully authenticated "tunnel" between the peer applications without the need to modify any of the sockets, TDI protocols, or hardware drivers on either of the client computers'*. This portion of CHEN does not disclose a receiving system that receives the confirmation receipt comprising authenticated file attributes, after authentication by the third party authenticator as recited in independent claim 1 or the related features recited in independent claim 21.

Additionally, at col. 9, lines 43-59, CHEN discloses *"the arrangement shown in FIG. 3 modifies the arrangement of FIG. 2 by adding a socket shim 50 between the socket 22 utilized by the authentication client software 20, the peer-to-peer applications 36 which also utilize the socket 20, and the authentication client software itself. The shim 50 operates by hooking or intercepting call initiation function calls 40 made to the socket and, in response thereto, having the authentication client software initiate communications with the authentication server 23, shown in FIG. 6, in order to carry out the authentication protocol, as will be discussed in more detail below. Shim 50 also causes files 41 intended for the TDI layer to be diverted to the authentication software for encryption based on the session keys generated during the initial communications with the authentication server, and transmission as encrypted files 51 addressed to the peer application, also shown in FIG. 6, which could also be an application on the application server 28"* (emphasis added).

Thus, the above-noted disclosure of CHEN is directed to a diversion of files internal to

the authentication software in the client for encryption and transmission to a peer. Here the term authentication software refers to the computer program in the client that communicates with the VPN Server to authenticate the client and to obtain encryption keys. CHEN does not teach that at least one file authentication is received from the third party authenticator as recited in independent claims 1 and 21. Accordingly, Applicants request reconsideration and withdrawal of the rejection of independent claims 1 and 21.

Applicants separately traverse the rejection of dependent claims 2 and 22. The Official Action asserts that CHEN discloses the features of dependent claims 2 and 22 at col. 11, lines 23-25. These teachings of CHEN are not directed to a file transfer of at least one file to be authenticated as recited in independent claim 1 or the related features recited in independent claim 21. Rather, these teachings of CHEN are an interception of function calls and routing of the initialization procedure through channel 61 to the authentication server on FIG. 6 for establishing communications between peer-to-peer applications. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of dependent claims 2 and 22.

Applicants separately traverse the rejection of dependent claims 3 and 23. The Official Action asserts that features recited in dependent claims 3 and 23 are disclosed in CHEN at col.11, lines 4-7. However, at col. 10, line 66 to col. 11, line 7 CHEN discloses "*[t]he overall system utilizing the authentication client software illustrated in FIGS. 3-5 is schematically illustrated in FIG. 6. The principal components of the overall system are the client computers containing software of the type illustrated in FIGS. 2-5, including client authentication software*

20 and shims 50, 53, and/or 55, and applications with communications capabilities (represented by applications 27, 36, 37, and 56 on one client, and application 45 on the other)”. Thus, this portion of CHEN is not directed to a transfer of file attributes or an identification of a device or user of the device. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of dependent claims 3 and 23.

Applicants separately traverse the rejection of independent claims 6, 11, 16 and 26, and dependent claims 4-5, 7-10, 12-15, 17-20, 24-25 and 27-31 over CHEN in view of BAKER. In this regard, a key word search of both CHEN and BAKER reveals that neither of these documents mentions any term, phrase or teaching such as “file authentication” or “authentication of files”. Accordingly, neither CHEN or BAKER is directed to a method, system or device for authentication of files in digital systems. Further, a key word search of both CHEN and BAKER reveals that neither of these documents so much as mentions confirmation, let alone a “confirmation request system”. Further, a key word search of both CHEN and BAKER reveals that neither of these documents so much as mentions a “third party” let alone a “third party authenticator”. Finally, a key word search of both CHEN and BAKER reveals that neither of these documents so much as mentions a “receipt” of any kind, let alone the related features recited in claims 4-20 and 24-31. Therefore neither CHEN nor BAKER, either separately or in combination, disclose a file authentication processing device or requesting a confirmation receipt from a third party authenticator authenticating the attributes of a file. Therefore, if the rejection of claims 4-20 and 24-31 over CHEN in view of BAKER is maintained, Applicants respectfully request with the next Official Action that the Examiner cite any teaching in either CHEN or

BAKER that he believes explicitly discloses or anticipates the features of a file authentication requesting device for requesting a digital receipt from a third party authenticator authenticating the attributes of a file.

Applicants separately traverse the rejection of independent claims 6 and 16. In this regard, the Official Action asserts that the features of independent claims 6 and 16 are disclosed by CHEN at FIGS. 6-7; col. 11, lines 16-49 and col. 9, lines 42-59. However, the cited portions of CHEN are essentially the same as those cited by the Official Action regarding independent claims 1 and 21. Thus, these portions of CHEN do not disclose processing requests for authentication of files in digital systems as in the invention to which independent claim 6 is directed. There is no teaching in these portions of CHEN of transferring attributes of at least one file to be authenticated to the third party authenticator.

CHEN further discloses, at col. 11, lines 29-36, “[s]erver 23 then opens a secured channel 63 to the authentication client software 20 associated with peer application 45 by performing the same mutual authentication procedure performed for the purpose of establishing channel 63, and once the channel is established with its own session key, transmits information using the channel 63 session key which allows the client to recreate the channel 60 session key for use in decrypting communications sent over channel 62”. The VPN Server as taught by CHEN performs mutual authentication procedures and produces session keys, but does not perform authentication of file attributes received from devices requesting file authentication. CHEN does not disclose a sending system that sends the confirmation receipt comprising authenticated file attributes to the requesting device, after processing by the third party

authenticator, as recited in the pending claims.

The Official Action acknowledges that CHEN does not disclose "processing comprising a unique digital characterization of the file attributes, assuring at least in part tampering and modification detection". However, the Official Action asserts that the above-noted features are disclosed at col. 9, lines 33-36 of BAKER. At col. 9, lines 33-36 BAKER discloses the "*meter is securely configured so that once keys are installed during manufacture, they can never be removed or determined outside the manufacturing environment without leaving physical evidence of tampering*". These teachings in BAKER refer to detection of physical tampering with the meter after manufacture, not detection of tampering with or modification of a file after third party authentication. That is, there is no mention in BAKER of a unique digital characterization of the file attributes. Accordingly, Applicants request reconsideration and withdrawal of the rejection of independent claims 6 and 16.

Applicants separately traverse the rejection of independent claims 11 and 26. The Official Action asserts that CHEN discloses features of claims 11 and 26 at Fig. 6, Fig. 7, col. 9, lines 42-59 and col. 11, lines 16-49. However, the cited portions of CHEN are essentially the same as those cited by the Official Action regarding independent claims 1, 6, 16, and 21. These documents merely refer to establishing a communications channel between a client and a server, and between clients as peers. Thus, these documents do not disclose processing requests for authentication of files in digital systems as recited in the pending claims. There is no teaching in these portions of CHEN to a device that transfers attributes of at least one file to be authenticated to the third party authenticator.

In this regard, the VPN Server as taught by CHEN performs mutual authentication procedures and produces session keys. However, the VPN Server in CHEN does not perform authentication of file attributes received from devices requesting file authentication. CHEN teaches sending session key information. Further, CHEN does not disclose a sending system that sends the confirmation receipt comprising authenticated file attributes to the requesting device, after processing by the third party authenticator, as recited in the pending claims.

The Official Action acknowledges that CHEN does not disclose "processing comprising a unique digital characterization of the file attributes, assuring at least in part tampering and modification detection". However, the Official Action asserts that BAKER discloses these features at col. 9, lines 33-36. At col. 9, lines 33-36 BAKER teaches "[t]he meter is securely configured so that once keys are installed during manufacture, they can never be removed or determined outside the manufacturing environment without leaving physical evidence of tampering". This teaching in BAKER refers to detection of physical tampering with the meter after manufacture, not detection of tampering with or modification of a file after third party authentication. However, there is no mention in BAKER of a unique digital characterization of file attributes, as recited in the pending claims. Accordingly, Applicants request reconsideration and withdrawal of the rejection of claims 1 and 26.

Applicants separately traverse the rejection of claim 27. In this regard, the Official Action asserts, at col. 11, lines 23-25, that the features of claim 27 are disclosed in CHEN at col. 11, lines 23-25. However, there is no specific teaching in BAKER or CHEN of the feature recited in claim 27. Since neither CHEN nor BAKER teach authentication of file attributes by a

third party authenticator, there is no combination of the teachings of CHEN and BAKER that produces the feature of claim 27. Accordingly, Applicants request reconsideration and withdrawal of the rejection of dependent claim 27.

Applicants separately traverse the rejection of dependent claims 7, 12, 17 and 28. In this regard, the Official Action asserts that CHEN discloses the features of dependent claims 7, 12, 17 and 28 at col. 11, lines 23-25. However, there is no teaching in BAKER or CHEN of the features of the above-noted claims. Since neither CHEN nor BAKER teach authentication of file attributes by a third party authenticator, there is no combination of the teachings of CHEN and BAKER that produces the above-noted features of these claims. Accordingly, Applicants request reconsideration and withdrawal of the rejection of dependent claims 7, 12, 17 and 28.

Applicants separately traverse the rejection of dependent claims 4, 8, 13, 18, 24 and 29. In this regard, the Official Action asserts that BAKER discloses the features of dependent claims 4, 8, 13, 18, 24 and 29 at col. 7, lines 50-52. However, BAKER discloses, at col. 7, lines 50-52, *“[i]f the key ID is new, then at 88 Oak Box 20 generates and encrypts a key, attaches the key ID, and then signs and sends the message to Steel Box 32”*. This refers to generation and exchange of a key ID from a domain archive and sending the key ID to another process in the manufacture of postage meters. However, this does not disclose the features recited in dependent claims 4, 8, 13, 18, 24 and 29. Since neither CHEN nor BAKER teach authentication of file attributes by a third party authenticator nor sending confirmation receipts, there is no combination of the teachings of CHEN and BAKER that produces the of these claims. Accordingly, Applicants request reconsideration and withdrawal of the rejection of dependent claims 4, 8, 13, 18, 24 and

29.

Applicants separately traverse the rejection of dependent claims 5, 10, 15, 20, 25 and 31. In this regard, the Official Action asserts that BAKER discloses the features of dependent claims 5, 10, 15, 20, 25 and 31 at col. 2, lines 1-9. However, at col. 2, lines 1-9, BAKER discloses that a *'digital meter provides evidence of the payment of postage by signing the postal information on the envelope with two "digital tokens." One digital token provides evidence to the postal service, and the second digital token provides evidence to the vendor, such as the assignee of the present invention. A digital token is a truncation of the result of encrypting indicia information including, for example, postage value, piece count, date of submission, and originating post office'*. These teachings in BAKER refer to printing a digital token on an envelop to provide evidence of payment to the postal service. However, these teachings do not disclose authentication of file attributes by a postal authority as recited in Applicants' claims. Accordingly, Applicants request reconsideration and withdrawal of the rejection of dependent claims 5, 10, 15, 20, 25 and 31.

Applicants separately traverse the rejection of dependent claims 9, 14, 19 and 30. In this regard, the Official Action asserts that BAKER discloses the features of dependent claims 9, 14, 19 and 30 at col. 17, lines 12-15. However, BAKER discloses, at col. 17, lines 1-15, that *"Key Management Computer 24 retrieves a domain master key record from the domain archive, takes a local time stamp and at 342 forwards information to Brass box 21 in message MI8. Brass Box 21 generates test tokens from the Domain Master Key record from the Domain Archive 74"*. The combined local time stamp and master key record is not a confirmation receipt containing the

date and time of authentication of authenticated file attributes nor an identification of a requesting device. Further, CHEN does not disclose a confirmation receipt comprising authenticated file attributes. Accordingly, no combination of CHEN and BAKER produces the features recited in dependent claims 9, 14, 19 and 30. Accordingly, Applicants request reconsideration and withdrawal of the rejection of dependent claims 9, 14, 19 and 30.

As set forth above, CHEN and BAKER do not disclose the features recited in Applicants' independent claims 1, 6, 11, 16, 21 and 26, whether considered alone or in any proper combination. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of each of independent claims 1, 6, 11, 16, 21 and 26, at least for each of the reasons set forth above. Applicants further submit that each of dependent claims 2-5, 7-10, 12-15, 17-20, 22-25 and 27-31 is allowable at least for depending, directly or indirectly, from an allowable independent claim, as well as for additional reasons related to their own recitations.

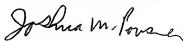
SUMMARY AND CONCLUSION

Applicants have made a sincere effort to place the present application in condition for allowance, and believe that they have now done so. Applicants have discussed the features recited in Applicants' claims and explained how these features are neither taught, disclosed, nor rendered obvious by any document cited in the Official Action. Accordingly, Applicants request an indication of the allowability of each of the claims now pending.

If there should be any questions concerning this application, the Examiner is invited to contact the undersigned at the telephone number listed below.

January 30, 2007
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

Respectfully submitted,
Maurice W. HAFF et al.

 Joshua M. Povsner
Stephen M. Roylance
Reg. No. 31,296
Reg. #42,086